UNITED STATES DISTRICT COURT
DISTRICT OF MONTANA

IN THE MATTER OF THE SEARCH OF INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE 1600 AMPHITHEATRE PARKWAY MOUNTAIN VIEW, CALIFORNIA 94043, ASSOCIATED WITH THE EMAIL ACCOUNTS FUN1JJ1978@GMAIL.COM AND NSAYLER@GMAIL.COM; THE IMEI 3529 1110 0163 379	AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Aaron Christensen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (hereinafter the "Provider"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United

States Code. I have been so employed by the FBI since May of 2009.

3. I have received training regarding the analysis of electronic communication providers' historical call detail records which includes using those records to identify and geo-spatially locate mobile devices.

4. The statements in this affidavit are based in part on information provided by law enforcement officers assigned to other law enforcement agencies, other Special Agents and employees of the FBI, and on my experience and background as a law enforcement officer as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a warrant from the Court, your Affiant has not included each and every fact known to me concerning this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 USC 2252(a)(2)(distribution of child pornography) have occurred. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of this crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. I have learned the following about the Provider:

BACKGROUND CONCERNING EMAIL

8. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. A Google subscriber can also store with the Provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

10. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information

may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

11. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

12. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

14. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device. A cellular telephone has a unique identifier associated with the device itself. The is often referred to as an IMEI (International Mobile Equipment Identifier) or MEID (Mobile Equipment Identifier. Google is able to identify and/or locate a given subscriber's account based on one of these identifiers.

15. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other

identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. Other sources of information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

19. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

20. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from sources including GPS data, cell site/cell tower information, and Wi-Fi access points.

21. Location data can assist investigators in understanding the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

EXAMINATION OF ELECTRONIC INFORMATION

22. The initial examination of the electronic information will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 120 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

23. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders responsive to this search warrant do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

24. If an examination is conducted, and the electronic information produced in response to this warrant does not contain any data falling within the scope of the warrant, the government will seal any non-responsive information, absent further authorization from the Court.

25. The government will retain a forensic image of all of the electronic information produced in response to this warrant for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

PROBABLE CAUSE

26. In September 2020, FBI Houston opened an investigation into a Kik user handle, "lvndad2grl." lvndad2grl had been observed online distributing files meeting the federal statutory definition of child pornography. In September 2020, lvndad2grl was subsequently arrested and his electronic devices were searched. During the review of the extracted material

recovered from lvndad2grl's telephone, multiple social media chats between lvndad2grl and various other Kik users to include Kik user handle, "vjayjayjohn," were discovered. lvndad2grl and vjayjayjohn messaged one another on Kik in a discussion in which lvndad2grl was obtaining advice from vjayjayjohn on how to operate a Kik chatroom and vet other users interested in joining the chatroom. A brief summary of the communication that took place in September of 2020 is provided below:

> vjayjayjohn advised that lvndad2grl request "daughter pics or young in general" as a way to get images from the chatroom applicants as part of the vetting process. vjayjayjohn then sends a picture of a female child, under the age of 5, in a pink one-piece bathing suit to lvndad2grl as an example. lvndad2grl responds, "Hopefully most are their real kids," to which vjayjayjohn responds, "I hope to I'm jacking to her". lvndad2grl writes, "Ever get active dads…" and vjayjayjohn responds, "Some". The conversation continues with lvndad2grl asking, "Question...any good active sites? How find kids". vjayjayjohn responds, "Your guess good as mine check out filter lots of kid porn being posted". vjayjayjohn then sends a video to lvndad2grl of two naked female children of approximately the age of 10. One of the girls is licking the navel of the other nude child that is laying on a bed. The girl that was licking the other girl then moves onto her hands and knees while the other girl massages her back and torso and spreads her gluteal cheeks exposing her anus and vulva for the photographer to zoom in and capture a closer image. lvndad2grl gets back to discussing the chatroom rules, "We should add..in rules to include member age/sex and daughter age." lvndad2grl continues to discuss rules and verification for the chatroom. vjayjayjohn asks, "Any flat chest girls". lvndad2grl suggests that vjayjayjohn add an application called "Mega," to his device. lvndad2grl then send an image of an approximately 5-year-old female only wearing bikini bottoms to vjayjayjohn. vjayjayjohn responds the following day that he likes the picture. lvndad2grl discusses that the chatroom is being visited by "Alot of fakes…many don't want to send live pic" and lvndad2grl indicates that he bans those from the room. lvndad2grl then sends an image of a clothed teenage female to which vjayjayjohn responds, "That's nice mmmm only the one?" vjayjayjohn mentions his daughter and lvndad2grl responds, "Oh very nice…Cute". vjayjayjohn responds, "Like showing her off…Let's see…Your not sharing". lvndad2grl responds with a video of an adult male inserting his partially erect penis into the vagina and anus of an approximately 3- to 4-year-old female child who is kneeling with her pants and underwear pulled down. The soundtrack of the video captures screams of pain from the child. vjayjayjohn responds, "I've seen that that vid before somewhere two pics they need…I like that vid to mmmm" appearing to move the

conversation back to vetting of the chatroom participants. lvndad2grl responds, "A lot are fake..send one but can't do live…i remove them and say when live then can join. I'm making everything legit". The captured chat comes to a close as vjayjayjohn appears to have banned someone from the chatroom providing the excuse to lvndad2grl that the person didn't respond to a request from the previous day. lvndad2grl then sends an image of an approximately 9-year-old boy and an 11-year-old girl, fully clothed. vjayjayjohn responds, "I'd like to have her," to which lvndad2grl responds, "Yes trying nude".

27. Information furnished by Kik revealed that the vjayjayjohn account was associated with email account "fun1jj1978@gmail.com." Furthermore, Kik disclosed that Kik's Registration Client Information included android-id, ef3fe919b6c67e10. An administrative subpoena to Google revealed that telephone number 406-672-4457 was associated with the email account, fun1jj1978@gmail.com. Additionally, the IP address to which the Google Terms of Service in relation to this email account were agreed to was 174.45.240.13. A subpoena to Charter Communications revealed that a known person, hereafter referred to as "Jane Doe" for privacy purposes, was the subscriber for this IP address. Furthermore, Google revealed that the email account, fun1jj1978@gmail.com, was accessed using IP address 2600:100e:b145:feaf:366e:fe25:207f:e9f3 in October of 2020. This IP address was determined to be a Verizon Wireless IP address. In response to a subpoena, Verizon Wireless revealed that during the timeframe that the phone accessed the email account, fun1jj1978@gmail.com, with IP address, 2600:100e:b145:feaf:366e:fe25:207f:e9f3, this IP address was assigned to Jane Doe's account and was associated with telephone number, 406-672-4457. Furthermore, this telephone number had been subscribed to by Jane Doe since May of 2020.

28. Jane Doe's ex-husband, NATHAN ALLEN SAYLER, had previously been charged and convicted by the State of Montana in Yellowstone County for Sexual Abuse of

Children. In 2018, SAYLER admitted to an Internet Crimes Against Children (ICAC) investigator, Billings Police Officer Earl Campbell, that he had used Kik communicate with a 14-year-old and had exchanged nude photographs with her.

29. An open-source check conducted by the FBI showed that SAYLER also uses or used gmail account nsayler@gmail.com.

30. On December 16, 2020, SAYLER was contacted, in-person, by State of Montana Adult Probation/Parole officer (PO), Krystal Stevenson, who was supervising SAYLER. SAYLER denied having any phones other than the flip phone that he had on his person. Information provided by Kik identified the SUBJECT PHONE as a Nokia 3 V smartphone. PO Stevenson contacted Jane Doe, who believed that the smartphone that she purchased for SAYLER and provided for his use, was located at her home in a drawer. Jane Doe relayed this information to PO Stevenson following a search of SAYLER's residence and vehicle for the SUBJECT PHONE, which was not located in this probation-directed search. PO Stevenson left the search and traveled immediately to Jane Doe's residence. On arrival at Jane Doe's residence, Jane Doe advised that SAYLER's smartphone was not located in the drawer.

31. Jane Doe confirmed to an FBI Special Agent that she had purchased the Nokia 3 V smartphone at SAYLER's direction, from Verizon Wireless, because he claimed to have needed the device to search for car parts on the internet. Jane Doe provided the telephone number, 406-672-4457, and provided the IMEI, 3529 1110 0163 379, for the device that she provided to SAYLER. SAYLER last spoke with Jane Doe on SAYLER's smartphone during the previous evening, December 15, 2020, and this previous evening's conversation was documented in Jane Doe's call log on her telephone.

32. At the time of the probation-authorized search of SAYLER's residence, SAYLER was interviewed by Billings Police Officer Earl Campbell and SA Walter. SAYLER initially stated that he communicated with Jane Doe on the flip phone that he had already provided to PO Stevenson. SAYLER was asked about the Nokia 3 V smartphone and stated, "What do you want me to tell you…I don't have it…I don't have it...I haven't had it in quite a while." SAYLER then admitted to obtaining the Nokia 3 V smartphone in June of 2020 from Jane Doe. SAYLER used the phone to communicate with Jane Doe, but stated that he had thrown the phone into the Yellowstone River in September of 2020. SAYLER denied using Kik since the time that he had previously gotten into trouble over his use of the application. SAYLER also denied knowledge of the email address, fun1jj1978@gmail.com.

33. On December 18, 2020, SA Walter spoke with Jane Doe on the telephone. Jane Doe relayed that while she was being interview by SA Walter (following SA Walter's contact with SAYLER and the search of SAYLER's home), two days earlier, SAYLER told her that he drove by her house, noticed the law enforcement presence, and departed only to return later. When SAYLER returned, Jane Doe went on a drive with SAYLER, during which he disclosed that after officers and agents departed the search of his house, he destroyed the phone that law enforcement was looking for. SAYLER didn't tell Jane Doe where he had the phone hidden on his property during the search, nor would he tell her how or where he destroyed the phone.

34. On March 16, 2023, SAYLER was indicted by a Montana Grand Jury with the Distribution of Child Pornography and Receipt of Child Pornography, in violation of 18 U.S.C. § 2252(a)(2). He was also charged with Destruction and Removal of Property to Prevent Seizure, in violation of 18 U.S.C. § 2232(a). This matter, which is currently pending trial, is reflected in

CR 23-31-BLG-SPW. The conduct underlying this Indictment is reflected in the paragraphs above.

35. On December 27, 2023, SAYLER moved to continue the trial date arguing, in part, "that Google location information would be vital to this case." Doc. 63 at 2. SAYLER argued that the government was the only entity able to access this information from Google. Doc. 64 at 4. On December 27, 2023, the Court granted SAYLER's motion to continue and reset trial for March 25, 2024. Doc. 64.

36. Because SAYLER denies having the SUBJECT PHONE in his possession at the time Kik users lvndad2grl and vjayjayjohn exchanged the child pornography, and because SAYLER himself claims that this information is vital to the pending criminal matter, it is necessary to obtain geolocation data for any devices linked to the Gmail account fun1jj1978@gmail.com during the relevant period. It is also necessary to obtain geolocation for SAYLER's alternate account nsayler@gmail.com, to determine whether exculpatory or inculpatory evidence exists to show SAYLER's location during the relevant period.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Aaron Christensen
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 17th, 2024

TIMOTHY J. CAVAN
UNITED STATES MAGISTRATE JUDGE